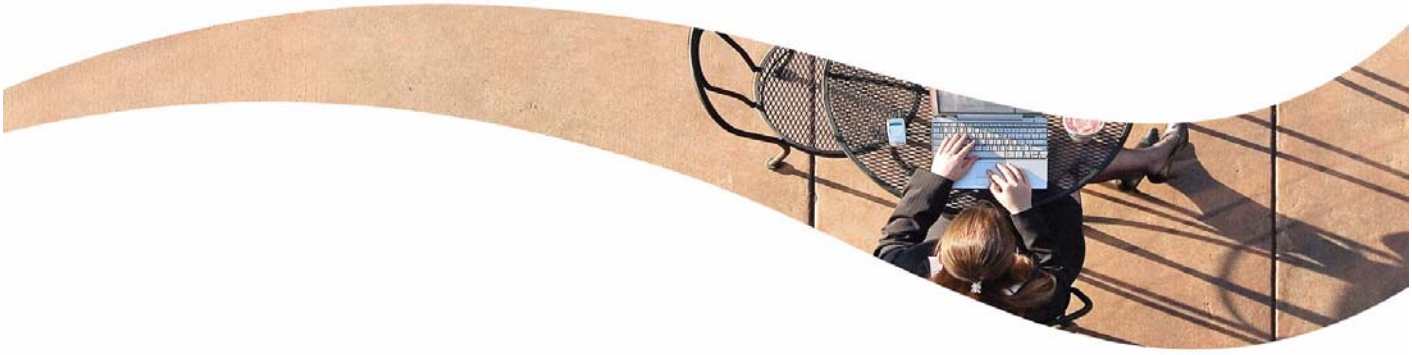


Configuring PortShield™ Interfaces

Document Scope

This document provides a feature overview and deployment configuration examples on configuring the SonicWALL Portshield Interface feature. This document contains the following sections:

- "Feature Overview" on page 1
- "Using PortShield Interfaces" on page 3
- "Deploying PortShield Interface Example" on page 4
- "Related Features" on page 32
- "Glossary" on page 33

Feature Overview

This section provides an introduction to the PortShield Interfaces feature. This section contains the following subsections:

- "What is SonicWALL PortShield Architecture" on page 2
- "Benefits" on page 3
- "Platforms" on page 3
- "Supported Standards and RFCs" on page 3

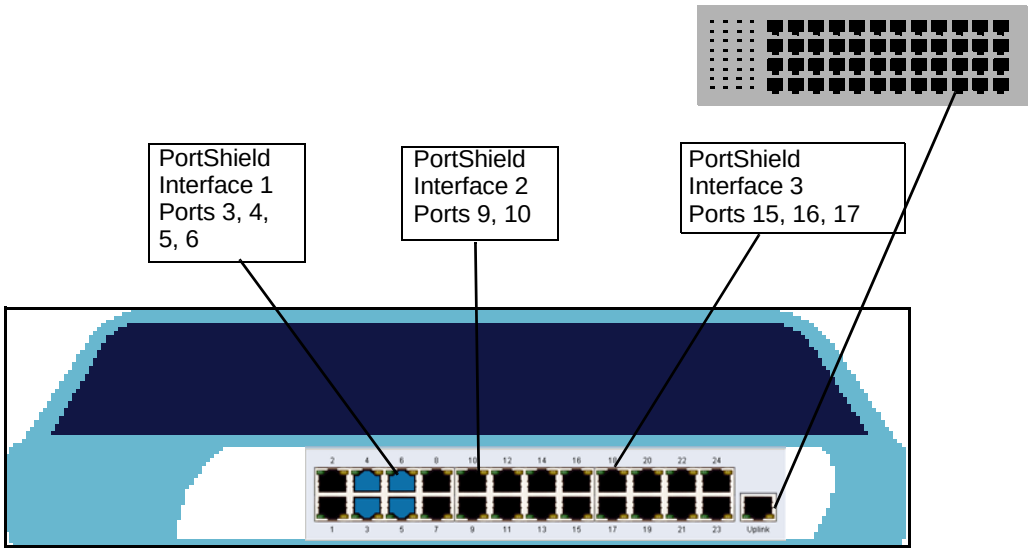
What is SonicWALL PortShield Architecture

The SonicWALL PortShield feature enables you to configure some or all of the 24 LAN switch ports on the SonicWALL PRO 1260 into separate contexts or *PortShield interfaces*, providing protection from traffic on the WAN and DMZ, and devices inside your network. Each context has its own wire-speed switch ports that have protection of a dedicated, deep packet inspection firewall.

You can assign any combination of ports on the SonicWALL PRO 1260 into a PortShield interface. By default, all 25 ports are part of the primary LAN interface. All ports you do not assign to a PortShield interface remain assigned to the LAN interface. For example, if you assign ports 4 through 12 to a PortShield interface, ports 1 through 3, ports 13 through 24, and the Uplink port all remain assigned to the LAN interface.

You can create standard SonicWALL address objects and assign them to a PortShield interface, harnessing the convenience of using single objects to apply ranges or groups of non-consecutive addresses to a PortShield interface. For ranges and hosts, you conveniently can create the address object inside the PortShield interface creation environment.

You cannot assign Port 1 and the Uplink Port to a PortShield interface. They can only be part of a LAN interface. The following figure shows a basic view of what three PortShield interfaces on one device might look like.



SonicWALL PRO 1260

Benefits

The benefits of PortShield interfaces are:

Increased Manageability

- Provides a helpful organization mechanism that enables you to easily group ports into logical units reserved for topically-related traffic.
- Enables software configurations to be made uniform across devices by collapsing like resources into a single subnetwork. As an example, using PortShield interfaces can reduce the number of implementations of local server resources like DHCP.

Increased Performance

- Provides improved traffic efficiency by enabling you to reserve port groups for more demanding traffic and other port groups for less demanding traffic.
- Provides improved traffic efficiency by enabling you to group users into logical networks by limiting traffic to users performing similar functions, improving efficiency.

Increased Security

- It enables you to block designated ports from accepting sensitive information, segmenting the ports from more general traffic targeted for other ports which may be more prone to performance degrading packet analysis, and filtering mechanisms.
- It enables you to insulate designated ports from distressed segments experiencing flutter or that have failed, reducing the potential for data loss, degraded data, and floods of error messages.

Platforms

The PortShield interface feature is available on the SonicWALL PRO 1260 running SonicOS Enhanced version 3.1 or newer.

Supported Standards and RFCs

The SonicWALL PortShield interface technology feature supports the IEEE 802.1q standard, although 802.1q-based VLAN support is not available to the SonicWALL PRO 1260 as a user-controllable function. 802.1q tags are used internally by the PortShield interface function to direct packets to the correct interface after they enter the device.

The SonicWALL PortShield interface technology is based on the following RFCs, IEEE and other standards documents:

- ISO/IEC 15802-3
- IEEE 802.1q VLAN Tagging draft

Using PortShield Interfaces

This section contains the following subsections:

- “Prerequisites” on page 4
- “Configuration Tasks” on page 4

- "Configuration Outlines" on page 5
- "Understanding IP Assignment Modes" on page 6
- "Understanding IP Assignment Modes" on page 6
- "Creating a New Zone for the PortShield Interface" on page 9
- "Mapping Ports from the Switch Ports Window" on page 12
- "Verifying the PortShield Interfaces" on page 13
- "Creating Transparent Mode PortShield Interfaces" on page 14

Prerequisites

Prerequisites for configuring a PortShield interface are:

- You have a SonicWALL PRO 1260 running properly and all ports are in working order.
- Port 1 and the Uplink port need to be enabled.
- All other ports must meet two conditions: they must be enabled and have both the HTTP and HTTPS management options enabled that allow a management session to be established between the interface they map to and a network console.

When configuring a PortShield interface, you must configure the following elements:

- **Zone.** You must configure a zone either as Trusted, Public, or Wireless zone types.
- **Name.** You must assign a name to a PortShield interface.
- **Address Assignment Mode.** The manner in which the interface receives its IP address.
- **IP Address/Subnet Mask.** You must supply a unique IP address in non-overlapping subnetwork space. Assignments to a trusted or public zone allow for either Transparent or Static addressing. Assignments to a wireless zone continue to require a minimum of eight bits for host addressing.

Configuration Tasks

You can configure a PortShield interface in three ways.

- **Interfaces and Port Mappings in Two Sessions.** You can configure a PortShield interface first from the Interfaces environment and then by mapping ports to it in either of the two portions of the SwitchPort environment:
  - by selecting ports in the device graphic.
  - by clicking on the pen and paper icon in the switch ports list in the Configure column.

  By separating interface creation and switch port selection, you can focus more on each task. The Switch Port environment provides a graphical representation of the SonicWALL PRO 1260 interfaces. This provides an easy way to visualize where ports reside and how intuitive it will be to have certain ports grouped together into one PortShield interface. By having the interface already configured in a previous session, you can focus more on how to set up your different domains.
- **Interfaces and Port Mappings in One Session.** You can configure a PortShield interface and map ports to it both in the Interfaces environment. This approach provides the advantage of being able to quickly complete the configuration in one session in one environment. SonicOS provides an easy-to-use, tabbed environment to perform both tasks in the same session.

- **PortShield Interface Wizard.** By using the PortShield interface wizard and clicking on options presented in the wizard screens.

Configuration Outlines

The following task outlines detail the different tasks involved in the three methods of PortShield interface creation.

From the Interfaces Environment Only

To create a PortShield interface by configuring an interface and selecting ports to map to the interface in the interface environment, you perform the following tasks:

1. Establish a management session with the SonicWALL PRO 1260 device and access the Interfaces environment.
2. Create and add a PortShield interface to the list of interfaces. After you select a zone, you select a series of ports that you want to assign to the PortShield interface. You then select a method of IP address assignment.
3. Complete the configuration of the interface settings.

From Both the Interfaces and Switch Ports Environments

To create a PortShield interface using the from both the interface and switch ports environments, you perform the following tasks:

1. Establish a management session with the SonicWALL PRO 1260 device and access the Interfaces environment.
2. Create and add a PortShield interface to the Interface list.
3. Go to the Switch Port environment and assign ports to the PortShield interface you created.
4. You can select ports for your PortShield interface in one of the following ways:
   - from the device graphic.
   - from the dialog box displayed by clicking on the pen and paper icon (the same dialog box displayed in the Interface environment).

From the PortShield Interface Wizard

To create a PortShield interface using the PortShield wizard, you perform the following tasks:

1. Establish a management session with the SonicWALL PRO 1260 device.
2. From one of the environments listed here, launch the PortShield interface wizard. You can select the PortShield interface wizard from one of the following environments:
   - the System > Status page - the default environment (Wizards button located in the top-right corner).
   - the Network > Interfaces page (Wizards button located in the top-right corner)
   - the Network > Switch Ports page (PortShield Wizard button located in the top-right corner)
   - the Wizards page (PortShield Interface Wizard radio button displayed by clicking on the Wizards option in the navigation pane)
3. Navigate through the wizard screens, selecting and verifying one of the options presented for switch partitioning, which divides the ports up into preset ranges and enables IP address assignment to the interface.

Understanding IP Assignment Modes

You can use two different types of address assignment modes to create PortShield interfaces. They are *Static* and *Transparent*. Each has benefits to it depending on the number of addresses you want to assign to a PortShield interface. The following two sections describe each.

Working in Static Mode

When you create a PortShield interface in Static Mode, you manually create an explicit address to be applied to the PortShield interface. All ports mapped to the interface are identified by this address. Static mode is available on interfaces assigned to Trusted, Public, or Wireless zones. This approach is appropriate if you are configuring only one address for a PortShield interface as it gives you more control over the address selected while not taking a lot of time to manually make the assignment.

!

Note When you create a PortShield interface in Static Mode, verify the IP address you assign to the interface is not already in use by another PortShield interface.

Working in Transparent Mode

Transparent Mode addressing allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address is the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.

!

Note Verify the IP address you assign to the PortShield interface is within the WAN subnetwork.

When you create a PortShield interface in Transparent Mode, you create a range of addresses to be applied to the PortShield interface. You include these addresses in one entity called an Address Object. Address Objects allow for entities to be defined one time and to be re-used in multiple referential instances throughout the SonicOS interface. When you create a PortShield interface using an address object, all ports mapped to the interface are identified by any of the addresses specified in the address range. This approach is appropriate when adding multiple addresses because it saves time and reduces the potential for address conflicts.

Note Each statically addressed PortShield interface must be on a unique subnetwork. You cannot overlap PortShield interfaces across multiple subnetworks.

Creating a PortShield Interface from the Interfaces Area

Before creating and adding a PortShield interface, think about why you are creating it and what role it will play in your network. To create and add a PortShield interface to the list of interfaces, perform the following steps:

1. Click on the Interfaces option. The management software displays the Interfaces Settings screen.
2. Note the interfaces in the list contain the following columns of information:

Column	Description
Name	A string that identifies the interface.
Zone	The zone to which the interface maps.
IP Address	The IP address assigned to the interface.
Subnet Mask	The subnetwork mask value assigned to the IP address to indicate a range of addresses.
IP Assignment	The method in which the interface obtains its IP address: Static. Manually creating an explicit address to which you will map ports. Transparent. Allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address will be the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.

Column	Description
Status	Aggregate Ethernet Link port(s) status or Ethernet Link port(s) status summary, indicating the currently active highest speed and duplex properties.
Status	Aggregate Ethernet Link port(s) status or Ethernet Link port(s) status summary, indicating the currently active highest speed and duplex properties.
Comment	A note about the interface.
Configure	Contains two icons. One icon is a grouping of books that displays traffic statistics when you hover the mouse cursor over it. The other icon is a pen and paper that enables you to launch an interface configuration session.

3. Click the Add PortShield interface Settings button. The management software displays the Add Port Shield dialog box.
4. Click the Zone list box and click on a zone type option to which you want to map the interface. Default zones are:
   - LAN
   - DMZ
   - WLAN
   - Unassigned

   If you want to create another zone, go to the next section.

!

Note You can add PortShield interfaces only to Trusted, Public, and Wireless zones.

5. After you select a zone option, the management software displays a more expanded version of the PortShield Interface Settings dialog box.
6. Type a string (up to 32 characters long) in the PortShield Interface Name field that identifies the PortShield interface.
7. Click on the IP Assignment list box and click on either Static or Transparent. Static indicates the interface obtains its IP address manually. Transparent mode allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address will be the same as the WAN interface IP address.
8. Type an available IP address in the IP Address field.
9. If you want to specify a range of IP addresses different than the one allowed by the subnetwork mask 255.255.255.0 (Class C network), type in the desired subnetwork mask value in the Subnet Mask field.
10. Click on a checkbox in the Management area to indicate the desired management protocol type. The options are:
    - HTTP
    - HTTPS
    - Ping
    - SNMP

11. Click on a checkbox in the User Login area. This is a special feature that enables you to set up a Web access environment so you can enforce User Level Authentication. For more detail, see your SonicOS Administration Guide.
12. Click on the Create Default DHCP Lease Scope in the DHCP Server field to indicate that the amount of time allowed for an IP address issued by DHCP will be the default.

Note This option only appears when creating a PortShield interface, not when editing an existing PortShield interface. You can make changes to the interface's DHCP settings after creating an interface from the DHCP Server environment (Network>DHCP Server).

13. Click on the Switch Ports tab. The management software displays the PortShield Interface Ports dialog box.
14. In the Available Ports list, click on the port numbers you want to assign to the PortShield interface and click on the right arrow (->) button to move them into the Assigned Ports list.
15. Click Ok. The management software adds the PortShield interface to the interface list.

Creating a New Zone for the PortShield Interface

You may want to create a zone for a PortShield interface that has different attributes to it than any of the default zones provide. To create a new zone for a PortShield interface, perform the following:

1. Click on the Zone list box and click on the Create new zone option. The management software displays the General Settings dialog box.
2. Type a string in the Name field that will identify the new zone.
3. Click on the Security Type list box and click on a security type option that will classify the zone as having a certain level of access. The choices are:
   - **Trusted.** This security type offers the highest level of security, indicating that only trust, indicating that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the device. The LAN zone is always Trusted.
   - **Public.** This security type offers a higher level of security than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the device and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN.
   - **Wireless.** This security type applies to the WLAN zone or any zone where the only interface to the network consists of SonicWALL SonicPoint devices. You typical use WiFiSec to secure traffic in a wireless zone.
4. After selecting the security level for the PortShield interface, click on one of the checkboxes that enables a security service for the zone. The following table details:

Checkbox	Description
Allow Interface Trust	Automates the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance.
Enforce Content Filtering Service	Enforces protection and productivity policies for organizations to reduce legal and privacy risks while minimizing administration overhead.

Checkbox	Description
Enforce Network Anti-Virus Service	Enables network-level inspection of email, Web traffic, file transfers, various stream-based protocols, instant messaging, and peer-to-peer applications to detect and clean malicious code, viruses, and worms.
Enable Gateway Anti-Virus Service	Enables gateway-level inspection of email, Web traffic, file transfers, various stream-based protocols, instant messaging, and peer-to-peer applications to detect and clean malicious code, viruses, and worms.
Enable IPS	Enables Intrusion Prevention Service which provides a configurable, high-performance deep packet inspection architecture using parallel searching algorithms through the application layer to deliver complete Web and E-Mail attack prevention.
Enable Anti-Spyware Service	Enables spyware protection which prevents malicious spyware from infecting networks by blocking related installations at the gateway and disrupting background communications from existing spyware programs.
Enforce Global Security Clients	Enables the application of the SonicWALL Global Security Client that delivers comprehensive desktop security for remote/mobile workers and corporate networks.
Create Group VPNs	Enables group VPN creation.

5. Click Ok.

Refining the PortShield Interface

You can refine a PortShield interface group in the Switch Ports environment. To refine a PortShield interface group, perform the following steps:

1. Click on the Switch Ports option. The management software displays two major items:
   - a list of all interfaces including PortShield interfaces. Note the ports you have selected are parts of the PortShield interface you just created.
   - an interactive graphic of the ports on the switch
2. In the interactive graphic, click the ports for which you want to refine settings.
3. Click the Configure button. The management software displays the Edit Multiple Switch Ports dialog box. You can refine your settings in this dialog box.

   Note that the name of the PortShield interface group will be assigned by default.
4. Click on the Port Enable list box and click on either the Enable or Disable option to either activate or deactivate the ports in the PortShield interface group. Ports are enabled by default.
5. Click on the PortShield interface list box and click on an available PortShield interface.

6. Click on the Link Speed list box and click on a transmission and receiving speed you want to assign the interface. The choices are:
   - Auto negotiate
   - 100Mbps Full Duplex
   - 100 Mbps Half Duplex
   - 10 Mbps Full Duplex
   - 10 Mbps Half Duplex

   The link speed value indicates the transmission rate at which the device sends and receives packets to and from a sending device. The duplex variable indicates whether the connection between the SonicWALL PRO 1260 and the sending device allows concurrent transmissions from both devices.

Note Do not change this setting from the default of Auto negotiate unless your system requires you to do so. Also, note that for any setting involving the Full Duplex feature to work properly, be sure to configure Full Duplex on both ends of the link. By not having Full Duplex configured on both ends, a duplex mismatch occurs, causing throughput loss.

7. Click on the Rate Limit option and click on a value. The rate limit value enables you to throttle traffic coming into the switch. Remember, these values apply to inbound traffic only. The rate limit choices are:
   - 64 Kbps
   - 128 Kbps
   - 256 Kbps
   - 512 Kbps
   - 1 Mbps
   - 4 Mbps
   - 10 Mbps
   - 20 Mbps
8. Click Ok. Wait for a few seconds. The system then will incorporate the changes you made to the PortShield interface Group and add it back to the switch ports list.

Mapping Ports from the Switch Ports Window

Another way to create a PortShield interface is to configure the interface in the Interfaces window and then assign ports to it in the Switch Ports window. Approaching it this way assumes you created a PortShield interface first and then selected the ports from the device ports graphic and selected the existing interface. This provides several advantages:

- enables you to easily visualize the actual locations of ports.
- separating the task of creating the interface, helps you focus more on how you want to separate the ports into different domains.

To select ports and apply them to a previously configured interface, perform the following steps:

1. Either identify an existing PortShield interface that you want to map ports to or create a PortShield interface following the steps in the section previously described, but do not map ports to it by going into the Switch Ports tab.
2. Click the Networks > Switch Ports option. SonicOS displays the Switch Ports window.
3. Note the color of the ports. While you can map any port, no matter what its color, to an interface, you should be aware of whether it has been selected for use in another PortShield interface. Ports in different PortShield interfaces appear in different colors.
   - From the device graphic, see if any of the ports you want to select appear in black or another color. If a port is black, it is unused by another PortShield interface. If it is another color, it is in use by a PortShield interface. Just be cognizant of ones that are being used and what impact your remapping the port will have on the existing interface.
   - From the Switch Ports list, see if any of the ports in the PortShield Interface list have been selected as a PortShield interface.

   Be cognizant of ones that are being used and what impact your remapping the port will have on the existing interface.
4. On the device graphic, click on ports 3, 4, 5, and 6. The selected ports appear as yellow.
5. Click the Configure button. SonicOS displays the Switch Port Settings dialog box. Note the Name field displays the ports you selected (P3, P4, P5, P6).
6. Click on the PortShield Interface list box. Look for the PortShield interface name to which you want to map ports.
7. Click on the PortShield interface entry to which you want to map ports. By selecting this entry, you mapped ports 3, 4, 5, and 6to it.
8. Click Ok. View the Status: field at the lower left portion of the window. It displays the following message:

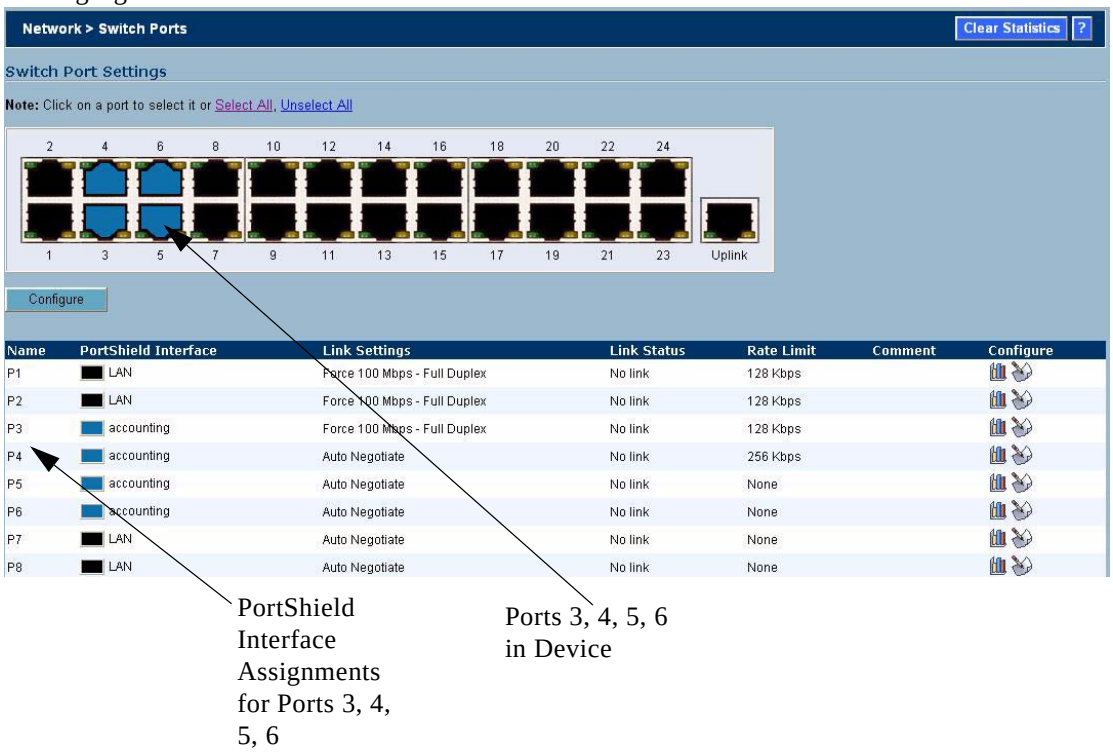
   Please wait

   The device takes a few moments while it adds ports to the PortShield interface. When the process completes, SonicOS displays the Switch Ports dialog box, displaying the results of your session. When the device completes adding the ports, it displays the following message:

   The configuration has been updated.

Verifying the PortShield Interfaces

SonicOS displays the Switch Ports dialog box, displaying the results of your session as shown the following figure.


Network > Switch Ports
Clear Statistics
Switch Port Settings
Note: Click on a port to select it or Select All, Unselect All
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23 Uplink
Configure
Name PortShield Interface Link Settings Link Status Rate Limit Comment Configure
P1 LAN Force 100 Mbps - Full Duplex No link 128 Kbps
P2 LAN Force 100 Mbps - Full Duplex No link 128 Kbps
P3 accounting Force 100 Mbps - Full Duplex No link 128 Kbps
P4 accounting Auto Negotiate No link 256 Kbps
P5 accounting Auto Negotiate No link None
P6 accounting Auto Negotiate No link None
P7 LAN Auto Negotiate No link None
P8 LAN Auto Negotiate No link None
PortShield Interface Assignments for Ports 3, 4, 5, 6
Ports 3, 4, 5, 6 in Device

Verify the PortShield interface port mappings. This example presupposes you have grouped ports 3, 4, 5, and 6 into a PortShield interface.

- In the device graphic, note SonicOS changed the color of ports 3, 4, 5, and 6from black to blue, indicating you successfully mapped them to a PortShield interface.
- In the Switch Ports list, view the PortShield Interface column for ports 3, 4, 5, and 6. This column now displays a blue-colored icon and the accounting string for P3, P4, P5, and P6, indicating these ports are now mapped to the accounting PortShield interface.

Creating Transparent Mode PortShield Interfaces

You may find it useful to create address objects to bundle addresses into address objects and reference these objects when creating a PortShield interface. Address objects allow for entities to be defined one time and to be reused in multiple referential instances throughout SonicOS. The PortShield interface creation environment provides a convenient way to reference address objects.

The following example takes a network with a series of addresses in the range 67.115.118.80/24 and divides it into three PortShield Interfaces, mapping each to the following ports and address objects:

PortShield Interface	Port Numbers Mapped	Address Object Type	Address(es)
portshield1	5	Address Object Host	67.115.118.90/32
portshield2	12, 13, 14	Address Object Range	67.115.118.100-67 .115.118.102
portshield3	16, 20	Address Object Host Group	67.115.118.200, 67.115.118.210, 67.115.118.212, 67.115.118.220, 67,115,118,230

To create these PortShield interfaces, using the prescribed address objects, perform the following steps:

1. Click on the Networks->Interfaces option. The management software displays the Interfaces Settings screen.
2. Click the Add PortShield Interface button. The management software displays the Add Port Shield dialog box.
3. Click the Zone list box and click on a zone type option to which you want to map the interface. For this exercise, click the LAN option. After you select a zone option, the management software displays a more expanded version of the PortShield Interface Settings dialog box. Only interfaces assigned to Trusted and Public zones can operate in Transparent mode.
4. Type a string in the PortShield Interface Name field.
5. Click on the IP Assignment list box and click the Transparent Mode option.
6. Click on the Transparent Range list box and click on the Create new address object option. The management software displays the Add Address Object dialog box.
7. Fill out the fields as detailed in the next three sections to create the three different types of address objects. The three scenarios presuppose you are in the 67.115.118.0 subnetwork.

Creating a Transparent Mode PortShield Interface with a Host Address Object

To assign the Host Address Object 67.115.118.90 to portshield1, perform the following steps:

1. Fill in the following fields:
   - Type the string portshield1 in the Name field to identify the address object.
   - Click the Zone Assignment list box and click the LAN option.
   - Click the Type list box and click the Host option to make the address object apply to a single IP address. Note the Host option is the default option in the list box.
   - Type 67.115.118.90 in the IP Address field. The management software presupposes a subnetwork mask of 255.255.255.255 (67.115.118.90/32). Note that because of this assumption, the software does not display a field for a subnetwork mask. Also, the field does not allow you to type enough a /32 notation as part of the address.
2. Click Ok. The management software displays the General tab of the Port Shield dialog box.
3. Click the Switch Ports tab. The management software displays the Switch Ports tab.
4. Click on P5 in the Available Ports list and click the right arrow (->) button to move the port into the Assigned Ports list.
5. Click Ok. The management software displays the Interfaces list displaying the new PortShield interface in the list. Note it displays the name, zone, IP address, subnetwork mask, IP assignment method, status, and comment, and link type status information about the address object you created (portshield1).

Note Note that the IP address is the actual subnetwork address, not the specific address you entered. In this example, the address is 67.115.118.0 and not 67.115.118.90. This is because in Transparent mode, the interface appears to users as having the same address as the gateway. Therefore your explicit address is invisible or transparent to Internet users. It lets you keep assigned IP addresses in the WAN subnet while protecting those hosts with full SonicWALL firewall protection (including services, etc.).

6. Click on the Switch Ports option in the left navigation pane.
   - In the graphic of the switch, view port number 5 and verify that the port is colored blue.
   - In the switch port list, view the PortShield Interface column for P5 (port 5) and verify that the interface listed is portshield1.
7. Refine the configuration of the PortShield Interface. For details, go to your SonicOS Administration Guide.

Creating a PortShield Using an Address Object Containing an Address Range

To assign a Range Address Object with addresses extending from 67.115.118.100 to 67.115.118.102 to portshield2, perform the following steps:

1. Fill in the following fields:
   - Type the string portshield2 in the Name field to identify the address object.
   - Click the Zone Assignment list box and click the LAN option.
   - Click the Type list box and click the Range option to make the address object apply to a range of addresses. The management software displays new fields in the Add Address Object dialog box.
   - Note the Starting IP Address and Ending IP Address fields in the dialog box.
   - Type 67.115.118.100 in the Starting IP Address field to establish this address as the minimum value in the range.
   - Type 67.115.118.102 in the Ending IP Address field to establish this address as the maximum value in the range.
2. Click Ok. The management software displays the General tab of the Port Shield dialog box.
3. Click the Switch Ports tab. The management software displays the Switch Ports tab.
4. Holding down the shift key, click on P12, P13, and P14, in the Available Ports list and click the right arrow (->) button to move the port into the Assigned Ports list.
5. Click Ok. Note the list displays the name, zone, IP address, subnetwork mask, IP assignment method, status, comment, and link type status detail about the address object you created (portshield2).
6. Click on the Switch Ports option in the left navigation pane.
   - In the graphic of the switch, view port numbers 12, 13, and 14, and verify the port is colored blue.
   - In the switch port list, view the PortShield Interface column for P12, P13, and P14 (ports 12, 13, 14) and verify that the interface listed is portshield2.
7. Refine the configuration of the PortShield Interface. For details, go to your SonicOS Administration Guide.

Creating a Transparent Mode PortShield Interface with a Group Address Object

To assign a Group Address Object with addresses 67.115.118.200, 67.115.118.210, 67.115.118.212 67.115.118.220, and 67.115.118.230 to portshield3, perform the following steps:

1. To add a Group Address Object, you need to go to the Address Objects window under Networks > Address Objects.
2. Click on the Add button in the Address Objects list in the window. SonicOS displays the Add Address Object dialog box.
3. Fill in the following fields:
   - Enter the string portshield3 in the Name field.
   - Select Network from the Type menu.
   - Enter 67.115.118.200 in the network IP address and 255.255.255.0 in the Netmask field.
   - Click on the Zone Assignment list box and click on LAN.

4. Click Ok. The Management Software displays the Address Objects window displaying the new portshield3 in the address group list.
5. Repeat the procedure with the same settings for the following IP addresses: 67.115.118.210, 67.115.118.212 67.115.118.220, and 67.115.118.230. Verify the name of the address object for each address is portshield3. When you finish creating these address objects, you will only see portshield3 displayed in the address group list.
6. Go back to the Add PortShield Interface dialog box and create an interface called portshield3 with a LAN zone, using a Transparent Mode address assignment type and select portshield3 from the Transparent Range list of existing address groups.
7. Click on the Switch Port tab and add the ports 16 and 20 to the address object.
8. Click OK. SonicOS displays the group address object portshield3 in the Interfaces list. Note the Network and Netmask fields in the dialog box. Also, view the following:
   - In the graphic of the switch, view port numbers 16 and 20, and verify that the port is colored blue.
   - In the switch port list, view the PortShield Interface column for P16 and P20 (ports 16 and 20) and verify that the interface listed is portshield3.
9. Refine the configuration of the PortShield Interface. For details, go to your SonicOS Administration Guide.

Creating a Transparent Mode PortShield Interface with a Group Address Object

To assign a Group Address Object with addresses 67.115.118.200, 67.115.118.210, 67.115.118.212 67.115.118.220, and 67.115.118.230 to portshield3, perform the following steps:

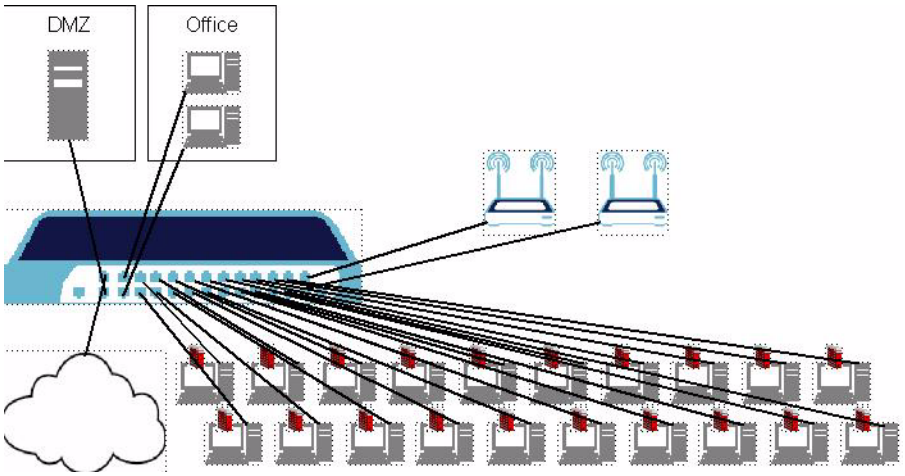
1. To add a Group Address Object, you need to go to the Address Objects window under Networks > Address Objects.
2. Click on the Add button in the Address Objects list in the window. SonicOS displays the Add Address Object dialog box.
3. Fill in the following fields:
   - Enter the string portshield3 in the Name field.
   - Select Network from the Type menu.
   - Enter 67.115.118.200 in the network IP address and 255.255.255.0 in the Netmask field.
   - Click on the Zone Assignment list box and click on LAN.
4. Click Ok. The Management Software displays the Address Objects window displaying the new portshield3 in the address group list.
5. Repeat the procedure with the same settings for the following IP addresses: 67.115.118.210, 67.115.118.212 67.115.118.220, and 67.115.118.230. Verify the name of the address object for each address is portshield3. When you finish creating these address objects, you will only see portshield3 displayed in the address group list.
6. Go back to the Add PortShield Interface dialog box and create an interface called portshield3 with a LAN zone, using a Transparent Mode address assignment type and select portshield3 from the Transparent Range list of existing address groups.
7. Click on the Switch Port tab and add the ports 16 and 20 to the address object.
8. Click OK. SonicOS displays the group address object portshield3 in the Interfaces list. Note the Network and Netmask fields in the dialog box. View the following:

- In the graphic of the switch, view port numbers 16 and 20, and verify that the port is colored blue.
- In the switch port list, view the PortShield Interface column for P16 and P20 (ports 16 and 20) and verify that the interface listed is portshield3.

9. Refine the configuration of the PortShield Interface. For details, go to your SonicOS Administration Guide.

Deployment Scenario

A SonicWALL PRO 1260 with PortShield can be used in a small hotel or apartment setting. For example, an apartment complex with 20 apartments could have a PortShield group for each individual room, two sonicpoints to give wireless access to residents, a small office LAN, and a mail and web server in a DMZ. With all SonicWALL Security Services enabled, the network behaves as if each apartment had a separate firewall.



!

Note The easiest way to configure this example is to use the PortShield Wizard. Configure it to have 24 PortShield interfaces, with one port each. Then reconfigure the LAN to include 2 ports and reconfigure the wireless group to include 2 ports. For more details on the PortShield Wizard, see the appropriate wizard chapter.

Configuration steps

This example has the uses the following zones and PortShield interfaces:

Zones

- **LAN**: Default LAN zone configuration.
  - Used for Office PortShield Group.
  - All SonicWALL Security Services enabled.
- **Residents**: A custom zone for the General Users PortShield group. Residents is a Wireless zone with SonicPoint Enforcement disabled so it can be used like a LAN with mixed wired and wireless clients.
  - Used for the Residents PortShield group.
  - Zone Type: Wireless
  - All SonicWALL Security Services enabled.
  - **Only allow traffic generated by a SonicPoint** is not checked, disabling SonicPoint Enforcement. This setting allows the zone to be used for both wired and wireless traffic.
  - **Enable Wireless Guest Services** is checked. With SonicPoint enforcement disabled, this enables both wired and wireless guest services.
  - **Enable Dynamic Address Translation (DAT)** is checked. With SonicPoint enforcement disabled, this enables DAT for both wired and wireless guests.
- **DMZ**: Default DMZ zone configuration.
  - Used for Opt port.
  - All SonicWALL Security Services enabled.

PortShield Groups

The small business example uses six PortShield interfaces.

- **LAN:** for office use
  - LAN zone
  - 2 ports, 1 - 2. These ports are assigned to LAN by not assigning them to another PortShield interface.
  - 2 desktop workstations
  - no wireless access
- Resident1 through Resident20
  - Resident custom Wireless zone with SonicPoint enforcement disabled
  - 1 port for each PortShield interface, from 3 to 24
  - One outlet in apartment
  - Wireless Guest Services enabled--both wireless and wired
- Wireless_Access
  - Resident custom Wireless zone with SonicPoint enforcement disabled
  - 2 ports, 23 - 24

  - Two SonicPoints connected, covering the whole complex and providing seamless roaming.
  - Wireless Guest Services enabled

Total 24 ports.

Configuring the Hospitality Example Deployment

Configuring the hospitality example deployment involves the following procedures:

- Configure the SonicPoint Profile
- Configure the Zones
- Configure the PortShield Interfaces with the PortShield Wizard
- Set Up the DMZ

Configure the SonicPoint Profile

This example uses two SonicPoints to grant wireless access to users throughout the complex. Residents can log in with their accounts, and guest users can log in using Wireless Guest Services. The SonicPoint profile contains the settings that the security appliance automatically applies to all connected SonicPoints.

Follow the procedures in the Administration Guide and configure the SonicPoint profile. Keep the defaults except where appropriate for your installation. Set the SSID for both 802.11a and 802.11g radios to a name that identifies the apartment complex or hotel, for example, “SonicWALL Arms Resident Internet.”

Configure the Zones

This example uses three zones inside its network, LAN, DMZ, and a custom zone, Residents. Residents is a Wireless zone with SonicPoint Enforcement disabled, thus allowing both wireless and wired access. Guest services is enabled, allowing both wired and wireless guest users access to the Internet.

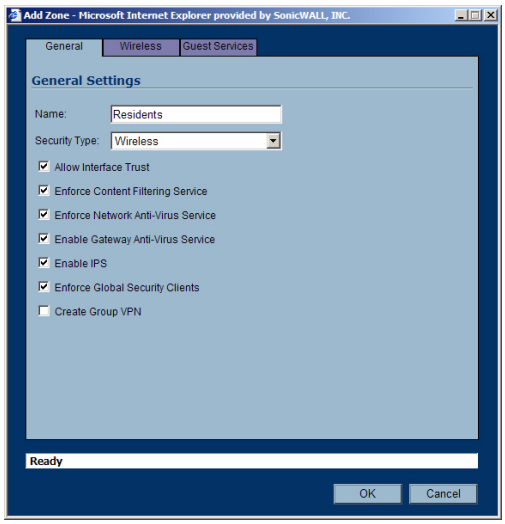
Configure the three Zones used in this example. Follow the procedures in the Zones chapter in your SonicOS Administration Guide.

LAN and **DMZ**: Leave the default configuration for these two zones.

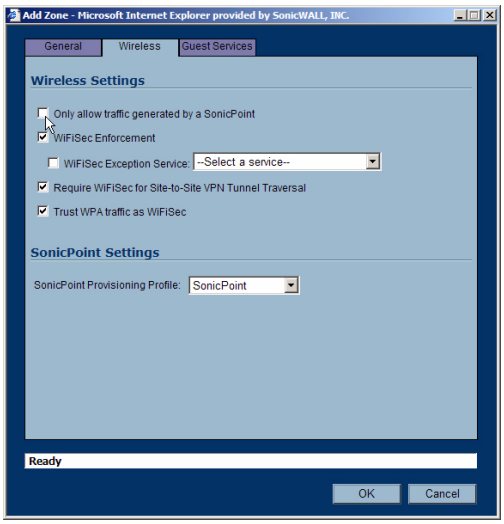
Residents: Configure the Residents zone with the following values:

- **General** tab settings:
  - **Name**: Residents
  - **Security Type**: Wireless. Select Wireless so you can use the same context for the both the individual wired connections and the SonicPoints.
  - **Allow Interface Trust**: Checked
  - **Enforce Content Filtering Service**: Checked
  - **Enforce Network Anti-Virus Service**: Checked
  - **Enable Gateway Anti-Virus Service**: Checked
  - **Enable IPS**: Checked
  - **Enforce Global Security Clients**: Only check if you want to require SonicWALL Global Security Client for your residents to log into the network.

– **Create Group VPN**: Only Check if you want to enforce WiFiSec security, requiring your residents to use a VPN client to connect.

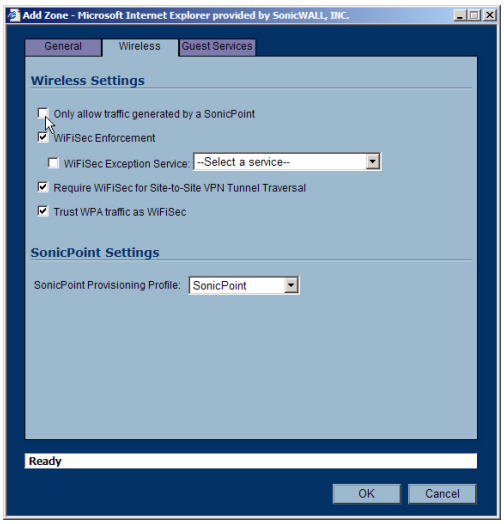


- **Wireless** tab settings:
  - **Only allow traffic generated by a SonicPoint**: Leave this option unchecked. This disables SonicPoint enforcement, allowing both wired and wireless connections through this zone.
  - **WiFiSec Enforcement**: Only check this option if you want to enforce WiFiSec security, requiring your residents to use a VPN client to connect.
  - **SonicPoint Provisioning Profile**: Select the SonicPoint profile you configured. The settings in this profile will automatically be applied to the SonicPoints you set up for wireless access.



- **Guest Services** tab settings:
  - **Enable Wireless Guest Services**: Check this option to enable access to the Internet for guest users who do not have resident accounts.
  - **Enable Dynamic Address Translation (DAT)**: Check this option to enable guest users to connect without having to change their Internet connection settings. See the Zones chapter in the SonicOS Administration Guide for more information on DAT.

– **Custom Authentication Page**: Only check this option if you want to create a custom login page for guest users.

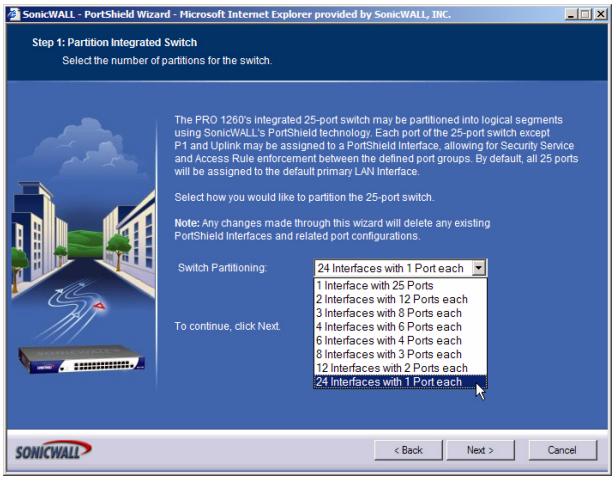


Configure the PortShield Interfaces with the PortShield Wizard

In this example, twenty apartments each have their own PortShield interface. Each of the twenty PortShield interfaces has a single port assigned to it. In addition, two ports are assigned to a Wireless PortShield interface for the SonicPoints. The Office has two ports assigned to the LAN interface.

The easiest way to configure this is to use the PortShield Wizard and then modify the configuration as follows:

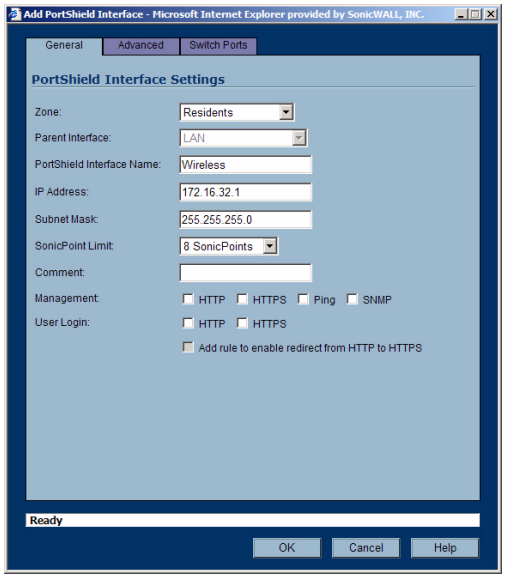
Use the wizard to configure 24 separate PortShield interfaces with one port each:


SonicWALL - PortShield Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
Step 1: Partition Integrated Switch
Select the number of partitions for the switch.
The PRO 1260's integrated 25-port switch may be partitioned into logical segments using SonicWALL's PortShield technology. Each port of the 25-port switch except P1 and Uplink may be assigned to a PortShield Interface, allowing for Security Service and Access Rule enforcement between the defined port groups. By default, all 25 ports will be assigned to the default primary LAN Interface.
Select how you would like to partition the 25-port switch.
Note: Any changes made through this wizard will delete any existing PortShield Interfaces and related port configurations.
Switch Partitioning:
24 Interfaces with 1 Port each
1 Interface with 25 Ports
2 Interfaces with 12 Ports each
3 Interfaces with 8 Ports each
4 Interfaces with 6 Ports each
6 Interfaces with 4 Ports each
8 Interfaces with 3 Ports each
12 Interfaces with 2 Ports each
24 Interfaces with 1 Port each
To continue, click Next.
SONICWALL
< Back
Next >
Cancel

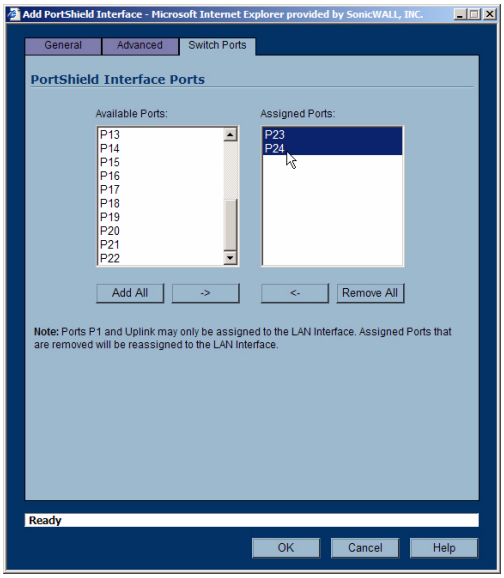
1. Launch the PortShield Wizard.
2. Select 24 PortShield interfaces with one port each.
3. Select to configure the PortShield interfaces automatically.
4. Create the interfaces.

Create the **Wireless_Access** PortShield interface for the SonicPoints.

1. In the Network > Interfaces page, click Add Interface.
2. Configure the Wireless_Access interface:
   - **Zone**: Residents
   - **PortShield Interface Name**: Wireless_Access
   - **IP Address**: 172.16.31.1 (or an appropriate address)
   - **Subnet Mask**: 255.255.255.0

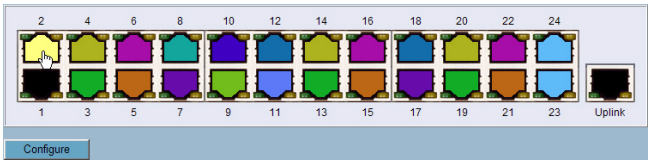


1. In the Switch Ports tab, assign ports 23 and 24 to the Wireless_Access PortShield interface.

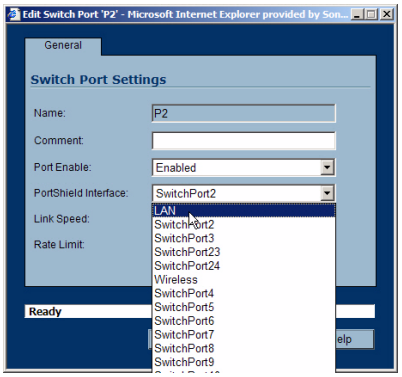


Use the Network > Switch Ports page to remove port 2 to the LAN interface

2. In the Network > Switch Ports page, select port 2 and click Configure.



3. In the Edit Switch Port page, Select LAN for the PortShield interface.



Set Up the DMZ

This example uses the Opt port as a DMZ for a mail and web server.

1. In the Network > Interfaces page, configure the Opt interface.
2. Select DMZ for zone.
3. Specify an appropriate IP address and network mask.

Small Business

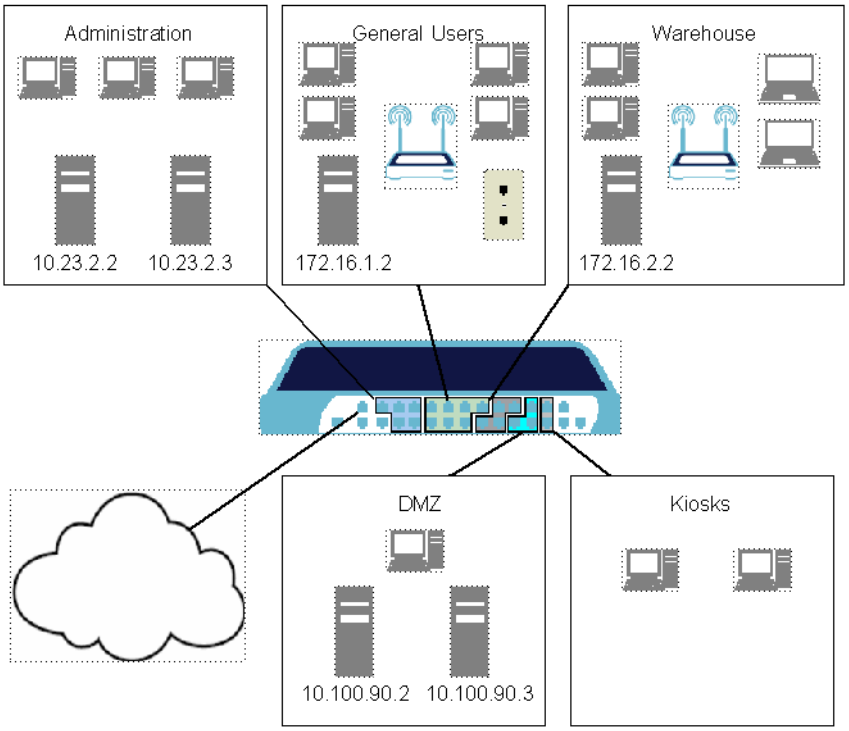
One good example deployment for PortShield interface groups is a small business office, with 25 or fewer clients on the network. PortShield allows the business to separate its network into contexts.

In this example, the network is divided into five zones, each served by a PortShield interface:

- Administration (including Accounting and Payroll) is on the LAN zone.
- General users in a custom Wireless zone. With SonicPoint Enforcement disabled, users in the company can have both wired and wireless access to the network. Wireless Guest Services is enabled to allow visitors to have both wired and wireless access to the Internet without access to the corporate network.
- Warehouse in a custom Wireless zone with SonicPoint Enforcement disabled. The warehouse has two stationary computers and warehouse users also have wireless access for handheld devices.
- The company has a DMZ for their mail server and Web server.
- Catalog kiosks are set up in the main building for customers to use. They are in a separate Kiosk zone.

All zones have the full array of SonicWALL Security Services enabled.

Note In the example, the ports are assigned to the PortShield groups in sequential order. However, you can assign any combination of ports to a group. If the company needs to expand the Administration group, they can add a combination of ports to a group. For example, if the company needs to expand, they can add either of the unused ports 23 or 24.



Small Business Example Configuration Details

Zones

- **LAN**: Default LAN zone configuration.
  - Used for Administration PortShield group.
  - All SonicWALL Security Services enabled.
- **General**: A custom zone for the General Users PortShield interface. General is a Wireless zone with SonicPoint Enforcement disabled so it can be used like a LAN with mixed wired and wireless clients.
  - Used for the General Users PortShield group.
  - Zone Type: Wireless.
  - All SonicWALL Security Services enabled.
  - Only allow traffic generated by a SonicPoint is not checked, disabling SonicPoint Enforcement. This setting allows the zone to be used for both wired and wireless traffic.
  - **Enable Wireless Guest Services** is checked. With SonicPoint enforcement disabled, this enables both wired and Wireless Guest Services.

  - **Enable Dynamic Address Translation (DAT)** is checked. With SonicPoint enforcement disabled, this enables DAT for both wired and Wireless Guest Services.
- **Warehouse**: A custom zone for the Warehouse PortShield interface. General is a Wireless zone with SonicPoint Enforcement disabled so it can be used like a LAN with mixed wired and wireless clients.
  - Zone Type: Wireless.
  - All Security services enabled.
  - **Only allow traffic generated by a SonicPoint** is not checked, disabling SonicPoint Enforcement. This setting allows the zone to be used for both wired and wireless traffic.
  - **Enable Wireless Guest Services** is not checked. Guest services is not enabled for the Warehouse zone.
- **DMZ**: Default DMZ zone configuration.
  - Used for DMZ PortShield Group.
  - All SonicWALL Security Services enabled.
- **Kiosk**: Copy of DMZ zone configuration.
  - Used for Kiosk PortShield.
  - All SonicWALL Security Services enabled.

PortShield Groups

The small business example uses six PortShield interfaces.

- Administration: for business office use, HR, Accounting, and Billing departments
  - LAN zone
  - 5 ports, 2 - 6
  - 10.100.23.0 subnet
  - Accounting, Billing, HR, etc.
  - Accounting Server 10.100.23.2
  - HR Server 10.100.23.3
  - 3 desktop workstations
  - no wireless access
- General Users
  - General custom Wireless zone with SonicPoint enforcement disabled
  - 7 ports, 7 - 13.
  - 172.16.1.0 subnet.
  - 4 desktops.
  - Server for sales software 172.16.1.2.
  - One SonicPoint for wireless access for employees.
  - Wireless Guest Services enabled--both wireless and wired.
  - One Guest port in conference room.
- Warehouse

  - Warehouse PortShield Group interface.
  - 4 ports, 14 - 17.
  - 172.16.2.0 subnet.
  - Mixed wired and wireless access.
  - Wireless Guest Services not enabled.
  - 2 fixed stationary computers.
  - 1 SonicPoint.
  - Wireless zone with SonicPoint enforcement disabled.
  - Inventory server 172.16.2.2.
- **DMZ**: for e-mail and Web and e-commerce Servers.
  - 3 ports, 18 - 20.
  - 10.100.90.0 subnet.
  - No Wireless Access.
  - Wireless Guest Services not enabled.
  - Mail Server 10.100.90.2.
  - Web Server 10.100.90.3.
  - Management station for servers - DHCP.
- **Kiosk**: for customer catalog kiosks.
  - 2 ports, 21 - 22.
  - 2 fixed stations with showing web interface of product catalog.
  - No Wireless Access.
  - Wireless Guest Services not enabled.

Total ports used: 21 - leaves 3 ports unassigned.

Configuring the Small Business Example Deployment

Configuring the Small Business example deployment involves the following procedures:

- Configure the SonicPoint Profile
- Configure the Zones
- Configure the PortShield Interfaces with the PortShield Wizard

Configure the SonicPoint Profile

This example uses a SonicPoint in the main office to grant wireless access to users throughout the company and a SonicPoint in the warehouse for wireless access from handheld devices like bar-code readers. WiFiSec is enforced so employees must log in with a VPN client. Guest access is available through the SonicPoint in the General zone.

Configure the SonicPoint profile according to the instructions in the *SonicOS Enhanced Administrator's Guide*. Keep the defaults except where appropriate for your installation. Set the SSID for both 802.11a and 802.11g radios to a name that identifies the network.

Configure the Zones

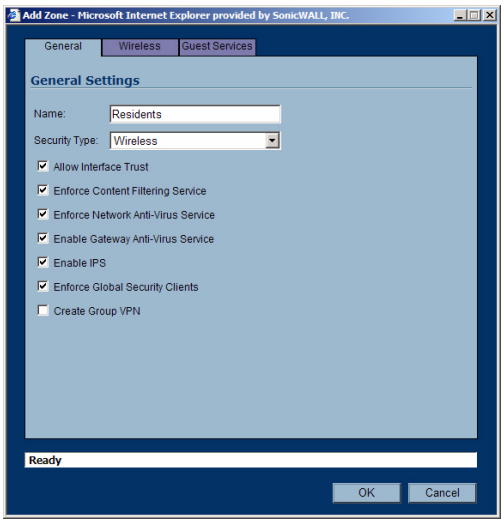
This example uses five zones inside its network, LAN, DMZ, General, Warehouse, and Kiosk.

Configure the five Zones used in this example. Follow the procedures in Chapter 14, Configuring Zones.

LAN and **DMZ**: Leave the default configuration for these two zones.

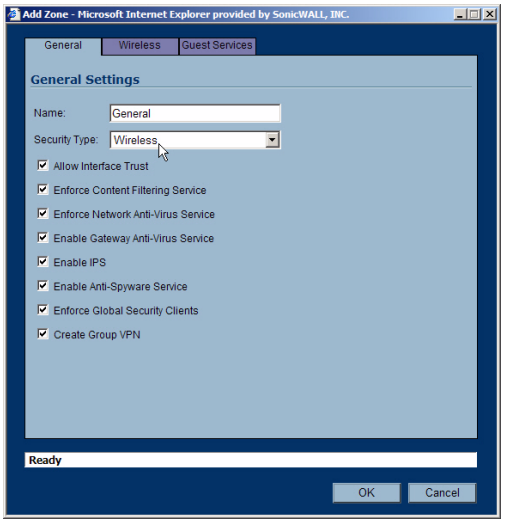
General: Configure the General zone with the following values:

- **General** tab settings:
  - **Name**: General
  - **Security Type**: **Wireless**. Select Wireless so you can use the same context for both wired connections and the SonicPoints.
  - **Allow Interface Trust**: Checked
  - **Enforce Content Filtering Service**: Checked
  - **Enforce Network Anti-Virus Service**: Checked
  - **Enable Gateway Anti-Virus Service**: Checked
  - **Enable IPS**: Checked
  - **Enforce Global Security Clients**: Check to manage SonicWALL Global Security Client settings
  - **Create Group VPN**: Check to provide a GroupVPN policy for users to log into when you enforce WiFiSec security.

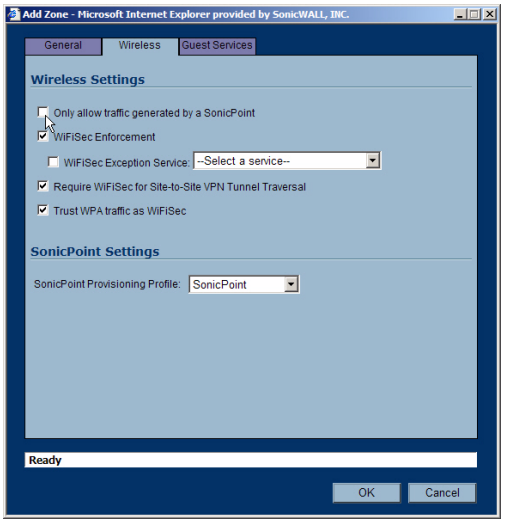


- **Wireless** tab settings:
  - **Only allow traffic generated by a SonicPoint**: Leave this option unchecked. This disables SonicPoint enforcement, allowing both wired and wireless connections through this zone.
  - **WiFiSec Enforcement**: Only check this option if you want to enforce WiFiSec security, requiring your residents to use a VPN client to connect.

– **SonicPoint Provisioning Profile**: Select the SonicPoint profile you configured. The settings in this profile will automatically be applied to the SonicPoints you set up for wireless access.



- **Guest Services** tab settings:
  - **Enable Wireless Guest Services**: Check this option to enable access to the Internet for guest users.
  - **Enable Dynamic Address Translation (DAT)**: Check this option to enable guest users to connect without having to change their Internet connection settings. See Chapter 14, Configuring Zones for more information on DAT.
  - **Custom Authentication Page**: Only check this option if you want to create a custom login page for guest users.



Warehouse: Configure the Warehouse zone with the following values:

- **General** tab settings:
  - **Name**: Warehouse
  - **Security Type**: **Wireless**. Select Wireless so you can use the same contexts for both wired connections and the SonicPoints.

  - **Allow Interface Trust**: Checked
  - **Enforce Content Filtering Service**: Checked
  - **Enforce Network Anti-Virus Service**: Checked
  - **Enable Gateway Anti-Virus Service**: Checked
  - **Enable IPS**: Checked
  - **Enforce Global Security Clients**: Check to manage SonicWALL Global Security Client settings
  - **Create Group VPN**: Check to provide a GroupVPN policy for users to log into when you enforce WiFiSec security.
- **Wireless** tab settings:
  - **Only allow traffic generated by a SonicPoint**: Leave this option unchecked. This disables SonicPoint enforcement, allowing both wired and wireless connections through this zone.
  - **WiFiSec Enforcement**: Only check this option if you want to enforce WiFiSec security, requiring your residents to use a VPN client to connect.
  - **SonicPoint Provisioning Profile**: Select the SonicPoint profile you configured. The settings in this profile will automatically be applied to the SonicPoints you set up for wireless access.
- **Guest Services** tab settings:
  - **Enable Wireless Guest Services**: Unchecked to disable Guest Services.

Kiosk: Configure the Kiosk zone with the following values:

- **General** tab settings:
  - **Name**: Kiosk
  - **Security Type**: **Public**.
  - **Allow Interface Trust**: Unchecked
  - **Enforce Content Filtering Service**: Checked
  - **Enforce Network Anti-Virus Service**: Checked
  - **Enable Gateway Anti-Virus Service**: Checked
  - **Enable IPS**: Checked
  - **Enforce Global Security Clients**: Unchecked
  - **Create Group VPN**: Unchecked

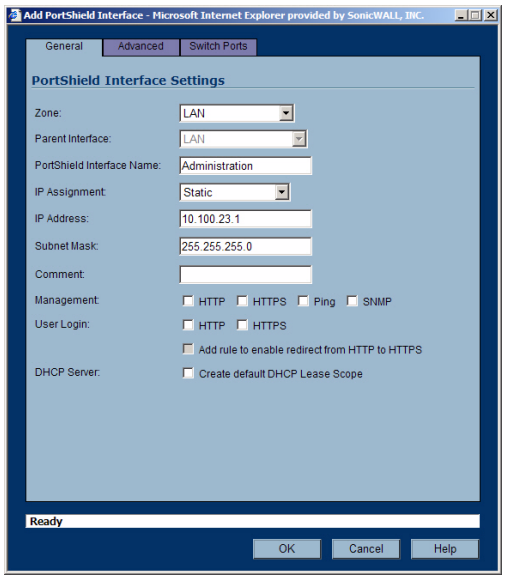
Configure the PortShield Interfaces

In this example, there are four PortShield interfaces, one assigned to the LAN zone, two assigned to Wireless zones (General and Warehouse) and one assigned to the Kiosk zone which is similar to a DMZ.

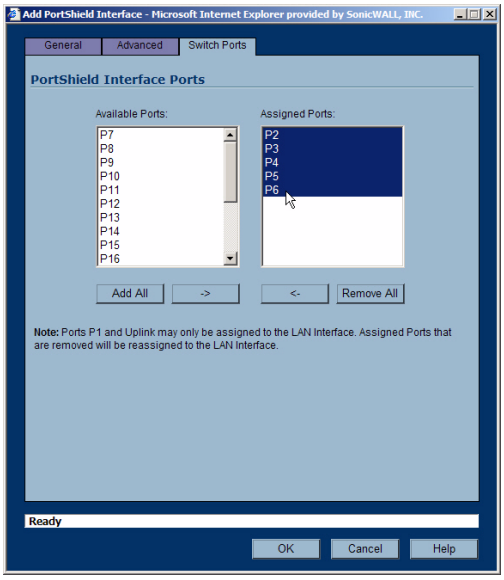
Create the **Administration** PortShield interface:

1. In the **Network** > **Interfaces** page, click Add Interface.
2. Configure the interface:
   - **Zone**: LAN
   - **PortShield Interface Name**: Administration
   - **IP Address**: 10.100.23.1 (or an appropriate address)

– **Subnet Mask**: 255.255.255.0



3. In the **Switch Ports** tab, assign ports 2 through 6 to the Administration PortShield interface.



Create the **General Users** PortShield interface:

1. In the **Network > Interfaces** page, click Add Interface.
2. Configure the interface:
   – **Zone**: General Users
   – **PortShield Interface Name**: General Users
   – **IP Address**: 172.16.1.1
   – **Subnet Mask**: 255.255.255.0
3. In the **Switch Ports** tab, assign ports 7 through 13 to the General Users PortShield interface.

Create the **Warehouse** PortShield interface:

1. In the **Network > Interfaces** page, click Add Interface.
2. Configure the interface:
   - **Zone**: Warehouse
   - **PortShield Interface Name**: Warehouse
   - **IP Address**: 172.16.2.1
   - **Subnet Mask**: 255.255.255.0
3. In the **Switch Ports** tab, assign ports 14 through 17 to the Warehouse PortShield interface.

Create the **DMZ** PortShield interface:

1. In the **Network > Interfaces** page, click Add Interface.
2. Configure the interface:
   - **Zone**: DMZ
   - **PortShield Interface Name**: DMZ
   - **IP Address**: 10.100.90.1
   - **Subnet Mask**: 255.255.255.0
3. In the **Switch Ports** tab, assign ports 18 through 20 to the DMZ PortShield interface.

Create the **Kiosk** PortShield interface:

1. In the **Network > Interfaces** page, click Add Interface.
2. Configure the interface:
   - **Zone**: Kiosk
   - **PortShield Interface Name**: Kiosk
   - **IP Address**: 10.100.100.1
   - **Subnet Mask**: 255.255.255.0
3. In the **Switch Ports** tab, assign ports 21 and 22 to the Kiosk PortShield interface.

Tip An alternative to configuring the Administration PortShield interface is to leave the ports unassigned. That way, they are automatically part of the LAN interface.

Related Features

- **Address Objects** - Use address objects to group addresses into ranges and address groups.
- **VLANs** - Use VLANs to deploy the IEEE 802.1q standard to group ports.

Glossary

- **802.1q** - An IEEE standard developed to address the problem of how to break large networks into smaller parts so broadcast and multicast traffic would not obtain more bandwidth than necessary. The standard also helps provide a higher level of security between segments of internal networks. The 802.1q specification establishes a standard method for inserting virtual LAN membership information into Ethernet frames.
- **802.1q Tags** - Virtual markers assigned to a physical port on the device that indicate which collision domain or PortShield interface to which the port belongs.
- **Address Object** - An aggregation mechanism that allows entities to be defined one time and to be reused in multiple referential instances throughout SonicOS. PortShield interfaces enable you to take advantage of the convenience of address objects by allowing you to map them either to a previously created address object or to an object that you create during the PortShield interface configuration session. You need to be in Transparent Mode to assign an address object to an interface.
- **PortShield Interfaces** - A software mechanism in SonicOS that enables you to configure some or all of the 24 LAN switch ports on the SonicWALL PRO 1260 into separate contexts, providing protection from traffic on the WAN and DMZ, and devices inside your network.
- **Primary LAN Interface** - The default base entity to which all ports on the SonicWALL PRO 1260 belong, acting as the single, collective interface on the device. You can select allowable ports in the Primary LAN to partition into separate PortShield interfaces that work separately but concurrently with the Primary LAN interface. The Uplink port and Port 1 are not allowable ports to be included in a newly created PortShield interface and always belong to the Primary LAN. By default, all standard addressing and zone assignment defaults apply to the Primary LAN.
- **Rate Limiting** - A limit that enables you to throttle traffic coming into the SonicWALL PRO 1260. By specifying a throughput value in SonicOS, you make that value fastest throughput rate by which incoming traffic can enter the device. This can be helpful in freeing an interface when it is overloaded with traffic, enabling it to operate more efficiently.
- **Static Mode** - A method of address assignment that allows you to explicitly assign a single address to a PortShield interface.
- **Transparent Mode** - A method of address assignment that allows for the WAN subnetwork to be shared by the current interface using Address Objects. The interface's IP address is the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.

PortShield Feature Module Version History

Version Number	Date	Notes
1	4/4/05	This document was created.